Riv. Mat. Univ. Parma (4) 5 (1979), 99-104

GIOVANNI FERRERO (*)

Osservazioni didattiche sulla divisibilità (**)

A GIORGIO SESTINI per il suo 70° compleanno

Introduzione

Come è noto i problemi dell'insegnamento dell'Algebra all'Università sono resi particolarmente complessi dal fatto che il corso del primo anno è l'unico corso algebrico seguito da tutti gli studenti, di modo che risulta difficile costruire un corso *organico* che li conduca (dalle poche nozioni intuitive ed imprecise che possono avere al primo impatto con l'Università) ad avere una idea di quello che è la moderna mentalità algebrica, al di là delle varie possibili specializzazioni.

Abbiamo dunque pensato di offrire al prof. Sestini, di cui ricordiamo brillanti conferenze didattiche tenute presso la Mathésis di Firenze, il tentativo di soluzione di questi problemi che vuole essere il corso che stiamo preparando esemplificando lo sviluppo di un argomento, come la teoria della divisibilità in semigruppi, molto importante sia dal punto di vista didattico sia per le sue applicazioni a semigruppi particolari. Esso risulta trattato qui in modo da richiamare, legare ed utilizzare più argomenti e tecniche di carattere generale mostrandone (almeno in parte) la portata, e permettendo confronti con le trattazioni di carattere pre-universitario.

Ovviamente, per brevità, possiamo limitarci a schizzare la trattazione omettendo le dimostrazioni e lasciando impliciti i presupposti: occorre tuttavia segnalare che reticoli ed anelli di Boole sono stati trattati in un capitolo introduttivo al corso propriamente detto, e che ad essi è seguita una trattazione dei

(*) Indirizzo: Istituto di Matematica, Università, 43100 Parma, Italy.

(**) Lavoro eseguito nell'ambito del G.N.S.A.G.A. (C.N.R.). — Ricevuto: 28-VI-1978.

primi elementi di algebra universale, riferiti al caso dei gruppoidi, in cui si è particolarmente insistito sui concetti di termine, interpretazione, identità e varietà.

Per la nomenclatura e le tecniche insiemistiche abbiamo seguito abbastanza strettamente [**3**], cui senz'altro rimandiamo per quanto di uso non del tutto universale.

1. – Sia $[S;\cdot]$ un semigruppo commutativo con unità. Le lettere latine minuscole indicheranno, ove non diversamente specificato, elementi di S. Diciamo che a divide b (e scriviamo $a\,|\,b$) se $\exists k\in S$ tale che $b=ka$. Senza la commutatività avremmo dovuto distinguere divisibilità destra e divisibilità sinistra. La relazione così introdotta è riflessiva e transitiva ma non di ordine parziale, come è in $\boldsymbol{N}$: possiamo, come in ogni caso simile, trarne una relazione di equivalenza. Diremo allo scopo che a è associato a b (e scriveremo aAb) se $a\,|\,b$ e $b\,|\,a$; la relazione A così introdotta è addirittura una congruenza in $[S;\cdot]$, perchè la divisibilità è compatibile con il prodotto. Possiamo allora considerare il gruppoide quoziente $[S/A;\cdot]$, che è ancora un semigruppo commutativo perchè i quozienti conservano le identità.

In S/A due elementi associati coincidono, di modo che la divisibilità è ivi una relazione di ordine parziale. Converrà quindi trattare dapprima la teoria della divisibilità in siffatto semigruppo, per poi passare a casi più generali usando l'omomorfismo canonico $\Phi\colon S\to S/A$. Predisporremo però alcune definizioni in modo che esse continuino ad avere interesse anche quando la divisibilità non sia una relazione di ordine parziale.

2. – Un elemento a di un semigruppo S si dice *irriducibile* se i suoi divisori non unitari sono ad esso associati; indicheremo con I l'insieme degli elementi irriducibili non unitari di S. Un $a\in S$ si dice *primo* se ogniqualvolta divide il prodotto cd di due elementi di S divide uno almeno dei fattori c, d; indicheremo con P l'insieme degli elementi primi non unitari di S.

Una sequenza $f\colon I_{(n)}\to S$ è detta *fattorizzazione* se $f(I_{(n)})\subseteq I$; se $a=\prod_i f(i)$ $(i\in I_{(n)})$ diremo che f è una fattorizzazione di a (una sequenza di lunghezza n è una funzione di dominio $I_{(n)}=\{1,2,\ldots,n\}$: termine ed abbreviazione si sono rivelati molto comodi anche altrove).

Diciamo che le fattorizzazioni f, f' sono equivalenti se esiste una biiezione $\varphi\colon I_{(n)}\to I_{(n)}$ tale che $f'=f\circ\varphi$. La relazione così definita risulta essere effettivamente una relazione di equivalenza (la più naturale dimostrazione risulta, con questa impostazione, interamente giocata sulla composizione di funzioni, ed è intuitiva senza cessare di essere strutturalistica). Due fattorizzazioni equivalenti sono fattorizzazione di uno stesso elemento di S, come risulta dal teorema generale di commutatività.

3. – Diciamo, per analogia col semigruppo moltiplicativo dei naturali, *intero* un semigruppo commutativo con unità tutti i cui elementi siano cancellabili ed in cui la relazione di divisibilità sia di ordine parziale. In questo numero, e nei successivi **4**, **5**, **6**, S sarà sempre un semigruppo intero ed S' il semigruppo dei suoi elementi non unitari.

Diciamo che S è *gaussiano* se (1) ogni elemento di S' ammette fattorizzazione, (2) due fattorizzazioni dello stesso elemento sono equivalenti.

Possiamo allora definire una funzione $l: S' \to \boldsymbol{N}$ che associa ad ogni $a \in S'$ la lunghezza delle sue fattorizzazioni. Si ha subito che se $a \mid b$ $(a, b \in S')$, allora $l(a) < l(b)$. Di qui scopriamo che se S è gaussiano in esso vale il cosiddetto criterio della catena, che cioè ogni successione $f: \boldsymbol{N} \to S$ tale che $\forall i \in \boldsymbol{N}$ ($\boldsymbol{N}$ insieme dei naturali zero escluso) sia $f(i+1) \mid f(i)$ e $f(i+1) \neq f(i)$ è una sequenza (ovvia formulazione abbreviata discussa in precedenza e su cui non possiamo dilungarci; essa è legata a notazioni e formulazioni insiemistiche di [**3**]). D'altra parte se in S vale il criterio della catena ogni elemento di S' è multiplo di un elemento di I ed anzi è fattorizzabile. Si ha poi che se S è gaussiano $I \subseteq P$. Abbiamo infine che un semigruppo intero S è gaussiano se e solo se (1) *in esso vale il criterio della catena*, (2) *ogni elemento irriducibile è primo.*

4. – Chiamiamo fattorizzazione ridotta in un semigruppo S una funzione $g: I \to \boldsymbol{N}_0$ ($\boldsymbol{N}_0$ insieme dei naturali zero incluso) tale che solo un numero finito di elementi di I abbia immagine diversa da zero. Se g è una tale fattorizzazione ridotta ha senso considerare il prodotto $\prod_i i^{g(i)}$ $(i \in I,\ g(i) \neq 0)$, e dire che g è una fattorizzazione ridotta di tale elemento.

Ogni elemento non unitario di un semigruppo gaussiano intero ammette una ed una sola fattorizzazione ridotta (una parte della dimostrazione è un esercizio sulla composizione di sequenze mediante giustapposizione e sul teorema generale di commutatività; la riteniamo particolarmente utile per mostrare come fatti sostanzialmente noti possano richiedere dimostrazioni complesse ove si voglia mantenere una linea rigorosamente insiemistica senza concedere nulla all'intuizione; ad ogni modo è utile confrontare la versione insiemistica con quella classica). Nel seguito del numero S sarà gaussiano intero.

Considerando ora la operazione di somma definita in $\boldsymbol{N}_0$ risulta automaticamente definita la somma di due fattorizzazioni ridotte g, g': $(g + g')(i) = g(i) + g'(i)$; si ha ancora una fattorizzazione ridotta, di modo che, detto F l'insieme delle fattorizzazioni ridotte, possiamo considerare il gruppoide $[F, +]$. Si ha anzi che la funzione Φ che associa ad ogni elemento di S' la sua fattorizzazione ridotta risulta essere un isomorfismo da $[S; \cdot]$ a $[F; +]$. Se, in S, $a \mid b$ allora, $\forall i \in I$, è $\Phi(a)(i) \leqslant \Phi(b)(i)$: proprietà che suggerisce di definire una relazione di confronto fra fattorizzazioni ridotte ponendo $g \leqslant g'$ se e solo se $g(i) \leqslant g'(i)$ $\forall i \in I$. Si ha così una relazione di ordine parziale « conservata »

dalla Φ (questo potrebbe essere uno strumento didattico per introdurre gli isomorfismi fra strutture d'ordine e per legare la trattazione « algebrica » della divisibilità che stiamo mandando avanti con una delle abituali trattazioni della divisibilità in semigruppi con cancellazione vista attraverso la teoria dei gruppi ordinati; noi, forse a torto, pensiamo più opportuno suggerire soltanto qualcosa in proposito a titolo di esercitazione, limitando lo studio teorico a quello di strutture direttamente riconducibili ai gruppoidi).

Ora è facile vedere mediante verifica diretta che i semigruppi gaussiani interi sono tutti e soli i gruppoidi isomorfi al prodotto diretto ristretto $[\boldsymbol{N}_0; +]^{(I)}$, con I insieme qualunque (a titolo di esercizio si potrà rileggere tutta la teoria per vedere quali delle proprietà segnalate sui semigruppi gaussiani interi vengano a cadere nel semigruppo $[\boldsymbol{N}_0; +]^I$).

5. – Se a, b sono elementi di un semigruppo S si dice *massimo comun divisore* di a, b ogni (eventuale) elemento di S che divida tanto a che b e sia multiplo di ogni divisore comune di a, b. In modo analogo si definiscono i *minimi comuni multipli*. Possiamo ora studiare questi concetti nei semigruppi gaussiani interi S: in essi, due qualunque elementi a, b ammettono uno ed un solo massimo comun divisore, che indicheremo con (a, b) ed uno ed un solo minimo comune multiplo, che indicheremo con $[a, b]$ (la dimostrazione si giova delle fattorizzazioni ridotte e del confronto in esse sopra definito, ed è la naturale versione insiemistica del procedimento elementare ben noto).

Un semigruppo gaussiano intero è anzi un reticolo distributivo rispetto alle operazioni $(\,,\,)$ e $[\,,\,]$ che sono state definite poco sopra.

Inoltre il prodotto è distributivo rispetto a tali operazioni: pertanto le $\alpha_a : S \to S$ definite dalla $\alpha_a : x \to ax$ sono endomorfismi per $[S; (\,,\,)]$ ed $[S; [\,,\,]]$.

Sempre con le fattorizzazioni ridotte si vede subito che in S vale l'identità $ab = (a, b)[a, b]$. Detti primi tra loro $a, b \in S$ se $(a, b) = 1$ si ha che in tale evenienza $ab = [a, b]$.

6. – Vogliamo ora mostrare che un semigruppo intero S è gaussiano se e solo se *in S vale il criterio della catena e due elementi qualunque di S ammettono massimo comun divisore* (l'analogo enunciato con l'ultima parte sostituita dalla « due qualunque elementi di S ammettono minimo comune multiplo » sembra invece, con la nostra impostazione, di non agibile dimostrazione (cfr. [4], p. 9)) Osservato infatti che se S è intero gli elementi a, b ammettono al più un massimo comun divisore, da indicarsi ancora con (a, b), possiamo condurre la dimostrazione attraverso osservazioni aventi anche interesse indipendente. Se S è intero è $c(a, b) = (ca, cb)$, purchè esistano (a, b), (ca, cb). Inoltre ora la $(\,,\,)$ risulta essere una operazione associativa e se $(a, b) = (a, c) = 1$ è anche $(a, bc) = 1$ (la dimostrazione del primo punto è diretta, quella del secondo

appena artificiosa; è utile confrontarla con le dimostrazioni degli stessi fatti per il caso gaussiano con il metodo ormai familiare delle fattorizzazioni ridotte). Di qui risulta che in un semigruppo intero, due cui elementi qualunque abbiano massimo comun divisore, ogni elemento irriducibile è primo, e il risultato fondamentale del n. **3** ci permette di giungere alla desiderata conclusione.

7. – Mettiamoci ora nelle condizioni di passare a casi più generali, in base a quanto visto nel n. **1**. Vale la pena di partire da un semigruppo commutativo S ed aggiungere via via condizioni su S che permettano di condurre l'operazione nel modo più semplice possibile.

Sia S un semigruppo commutativo ed A la congruenza definita nel n. **1**; indichiamo con $[a]$ l'elemento di A cui appartiene a. Fa chiaramente comodo che S/A abbia unità, non soltanto perchè a partire dal n. **3** abbiamo lavorato in semigruppi con unità (avremmo potuto evitarlo, e la variante senza unità può essere in parte vista come esercizio) quanto per avere un elemento di A su cui focalizzare la nostra attenzione, e tanto vale chiedere addirittura che S stesso abbia unità: si chiede così molto di più (vari esercizi avranno a suo tempo mostrato esempi di quozienti ed estensioni di Rees (cfr. per es. [**2**])); vuol dire che se dovesse essere utile cercheremo di generalizzare ancora, ma gli esempi che conosciamo ci dicono che chiedere che S/A abbia unità è, in fondo, chiedere molto poco.

In tali condizioni gli elementi unitari di S risultano essere precisamente gli elementi della classe $[1]$, e formano gruppo rispetto al prodotto.

Vogliamo ancora che in S/A tutti gli elementi siano cancellabili. Se è così e, in S, $a|b$ risulta (per opportuni $h, k \in S$) $a = hb$, $b = ka$, $a = hka$, $[a] = [hk][a]$, $[hk] = [1]$ e anzi $[h] = [k] = [1]$ di modo che possiamo dire che in S due elementi sono associati se e solo se differiscono per un fattore moltiplicativo unitario. Ma, visto che questa condizione non sembra sufficiente per garantire che tutti gli elementi di S/A siano cancellabili, chiediamo anche che in S stesso tutti gli elementi siano cancellabili. Allora per ogni classe $[a]$ di A la funzione $[1] \to [a]$ definita dalla $x \to ax$ è una biiezione, e possiamo scrivere $[a] = [1]\{a\}$ ove il prodotto a secondo membro è il prodotto di complessi, da cui la legge di cancellazione in S/A.

8. – Abbiamo dunque deciso di metterci in un semigruppo commutativo S con unità e legge di cancellazione, e di studiare la divisibilità in S, a partire da quanto sappiamo per S/A, usando l'omomorfismo canonico $\Phi: S \to S/A$: prepariamoci gli strumenti per farlo, dopo aver osservato che, come è ovvio, Φ conserva la divisibilità.

L'elemento $a \in S$ è irriducibile (primo) se e solo se lo è $[a] \in S/A$. Se $f: I_{(n)} \to S$ è una fattorizzazione di a in S, allora $\Phi \circ f$ è una fattorizzazione di $[a]$.

Se g è una fattorizzazione di $[a]$ esiste una fattorizzazione f di a tale che $g = \Phi \circ f$ (risulta utile confrontare le dimostrazioni di tipo tradizionale con quelle che esplicitamente vedono le fattorizzazioni come funzioni; è anche istruttivo contare le f tali che $g = \Phi \circ f$ per il caso in cui [1] sia finito).

Supponiamo ora che g, g' siano due fattorizzazioni equivalenti di $[a] \in S/A$. Noi possiamo trovare fattorizzazioni f, f' di a tali che $g = \Phi \circ f$, $g' = \Phi \circ f'$, ma non possiamo affatto dire che tali f, f' siano equivalenti. Se però chiamiamo essenzialmente equivalenti due fattorizzazioni f, f' di S quando $\Phi \circ f$ e $\Phi \circ f'$ sono equivalenti otteniamo una relazione di equivalenza (come si vede per ragioni insiemistiche elementari) che contiene l'equivalenza di fattorizzazioni di S. Notiamo che in S due fattorizzazioni dello stesso elemento risultino essenzialmente equivalenti se, e solo se, esiste una biiezione $\varphi: I_{(n)} \to I_{(n)}$ tale che, $\forall i \in I_{(n)}$, $f'(i)$ sia associato a $(f \circ \varphi)(i)$. In un semigruppo intero, ovviamente, equivalenza ed essenziale equivalenza coincidono.

Ora possiamo dire che S/A è gaussiano se, e solo se in S (1)′ *ogni elemento ammette fattorizzazione*, (2)′ *due fattorizzazioni dello stesso elemento sono essenzialmente equivalenti.* Questo, e quanto in precedenza osservato, suggerisce di modificare la definizione di semigruppo gaussiano chiamando così i semigruppi commutativi con unità e legge di cancellazione in cui valgano le (1)′, (2)′ di cui sopra, tanto più che questo non è in contraddizione con la definizione del n. **3**, che si riferiva ai semigruppi interi solamente.

9. – Osservato ancora che il criterio della catena vale in S/A se, e solo se, vale in S non resta che usare gli strumenti precedenti per rileggere gli enunciati dei numeri **3**, **4**, **5**, **6**, trovando gli ordinari risultati di teoria elementare della divisibilità in semigruppi commutativi con unità e con legge di cancellazione.

Bibliografia

[1] A. H. Clifford, *Arithmetic and ideal theory of commutative semigroups*, Ann. of Math. **39** (1938), 594-610.

[2] A. H. Clifford and G. B. Preston, *The Algebraic theory of semigroups*, Am. Math. Soc., Providence, Rhode Island 1961.

[3] C. Ferrero Cotti, S. Manara Pellegrini e A. Modena Suppa, *Insiemi e strutture*, Casanova, Parma 1978.

[4] P. Jaffard, *Les systèmes d'ideaux*, Dunod, Paris 1960.

Summary

A classroom presentation of the arithmetic of some semigroups.

* * *